National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Deployment Capability

Version 1.1.1

Deployment is the phase of the system development lifecycle in which solutions are placed into use to change or maintain the operational baseline. The Deployment Capability ensures that information assurance (IA) is employed while the processes for deployment are executed. When necessary, Deployment includes integration into the environment or other solutions and testing within that environment.

07/30/2012

CGS Deployment Capability
Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2   Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Deployment is the phase of the system development lifecycle in which solutions are placed into use to change or maintain the operational baseline. The Deployment Capability ensures that information assurance (IA) is employed while the processes for deployment are executed. When necessary, Deployment includes integration into the environment or other solutions and testing within that environment.

3   Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Deployment Capability is responsible for the incorporation of IA throughout the deployment phase of the lifecycle. The Capability is responsible for modifying and maintaining an operational baseline in accordance with mission needs.

The Deployment Capability includes coordination of security expertise and collaboration with the systems security engineers (SSEs), stakeholders, and developers who ensure the certification and accreditation (C&A) activities (see Risk Analysis Capability) and security requirements are defined to meet deployment IA objectives. This includes involvement of the Information Systems Security Officers (ISSOs) who shall be responsible for updating the system security plans and ensuring the overall secure deployment. The SSEs shall also ensure that the development, integration, and test personnel deploy systems securely by understanding the testing that was performed and the results, and understanding the changes that were made to the solution based on those test results. In addition, as part of the Deployment Capability, there shall be information technology (IT) support onsite at the time of deployment to ensure the process is executed properly. All personnel shall have the appropriate IA background and knowledge such that they can coordinate with the SSEs and ensure that the C&A and security requirements are understood, vetted, and accepted by the developers and

security stakeholders. The Capability shall employ services from a program management role or office to ensure that all activities and resources are managed according to the program management plan and are able to meet the established IA objectives. Program management shall also provide visibility into the deployment activity to other programs with dependencies on the deployment activity.

The Deployment Capability shall use the lifecycle process that is established and approved in accordance with the IA Policies, Procedures, and Standards Capability. The use of the established process ensures that deployment considerations are taken into account during the requirements process of the Development Capability. The security requirements that are the basis for deployment shall be defined in the development phase of the lifecycle.

An Enterprise shall perform a site survey to plan for a deployment. This site survey shall ensure that the site is ready and prepared for the deployment. Site surveys shall be not only for major deployments but also for understanding the deployment environment for smaller deployments, such as software packages. Deployment considerations shall include the necessary supporting infrastructure, such as space, power, and cooling, among other physical and environmental considerations. In addition, the survey shall ensure that onsite personnel have been trained for the solution that is being deployed at the operational site, and that access needs and points of contacts (POCs) have been identified.

As part of the Deployment Capability, special considerations shall be taken into account when deploying cryptographic devices and other specialized equipment. The transfer of specialized equipment shall use methods and accounting procedures as defined by the Enterprise's IA Policy, Procedures, and Standards Capability so that the appropriate plans are in place.

For Operational Security (OPSEC) and special security considerations for sensitive systems, the Enterprise shall deploy the systems in accordance with OPSEC policies or the policies uniquely defined for the sensitive systems. It may be necessary to use cover terms for protected sites. In these instances, ISSOs and security officials from the deployment site shall be consulted for security decisions when deploying such systems.

Proper deployment requires early notification to the site, customers, and owners of the solution that is scheduled for deployment. An Enterprise shall ensure that policies for collecting, storing, and processing data are in place before deployment occurs. Also, the

Enterprise shall review currently deployed corporate services to ensure corporate services are leveraged where appropriate and to ensure redundant services are not deployed. As part of this assessment, determining the value of a deployed solution is necessary for the Enterprise as well as for the considerations of the value for future needs. This shall ensure the resources that are needed for deployment are defined, along with the method(s) of deployment.

When systems are deployed, they shall be inventoried and provided shipping protections. An inventory of deployed capabilities, application of the necessary protections, and confirmation of inventory upon receipt shall be employed. Systems shall be shipped to the deployment site in accordance with Physical and Environmental Protection requirements. A pre-ship review and shipping audit shall be performed for the Deployment Capability. Stakeholders and security personnel shall approve the shipment prior to transfer for deployment. This shall ensure that all documentation, test results, discrepancy reports, permits, and certifications are in order. The pre-ship review and shipping audits shall have authorized approval for operation after deployment to the site. ISSOs shall be consulted for security decisions when deploying systems.

The Enterprise authorities and stakeholders shall make the final decision as to whether a solution will be deployed. As a basis for the decision, the deployment shall include documentation of the oversight and compliance requirements including any external measures and metrics. In addition, the deployment shall be coordinated with C&A activities and ultimately timed with the accreditation decision. As part of the C&A coordination, the C&A team shall report when systems are in danger of deploying without certain certifications. Subsequently, the stakeholders shall make any risk decisions based on the available information and the mission needs.

The Deployment Capability shall provide an operational mechanism that is certified and accredited for the Enterprise. Deployment shall include integration, installation, and, whenever feasible, testing at the operational site. Testing shall occur during deployment when feasible, to ensure that a deployed solution is functional and does not compromise the mission flow of an Enterprise. Because the integration of a capability takes place on the Enterprise's operational network, testing is not always optimal and may not happen. This decision shall be made on a case-by-case basis. If a deployed solution fails testing, procedures for uninstalling shall be defined, documented, and used to remove the solution or disable the solution for use on the Enterprise.

Once the solution is received and deployed at the site, the software and hardware assets shall be kept up to date. The hardware and software inventories shall be updated (see Hardware Device Inventory and Software Inventory) to reflect deployed hardware and software assets. The assets shall be configured to be discoverable by automated means, which allows for automated deployed updates and upgrades of operational technologies on the Enterprise.

During post-deployment, the solution shall be evaluated against the performance goals defined by the Portfolio Management Capability. This evaluation shall determine whether the deployed solution is operating effectively for the mission needs of the Enterprise.

4   Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Functional and security requirements were properly captured during development, and the solution has been verified and validated by the customer, end users, and system owner(s).
2. All solutions are thoroughly tested, simulated, or modeled prior to deployment, where possible.
3. A deployment plan is defined, which also documents the operations and maintenance plan.
4. The infrastructure will support the deployment.
5. Only authorized administrators can make approved system configuration changes during deployment.
6. All programs have an established program management role or office to manage activities and resources.

5   Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability coordinates with site administrators as part of the installation process.
2. The Capability stores records of system deployments in a central repository approved by SSEs.

3. The Capability provides a documented, approved, operational system.

6   Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When the Deployment Capability is implemented correctly, the Organization will possess a process for efficiently and effectively incorporating security throughout the deployment phase of the lifecycle. An Organization will use an approved and established process for deployment, which includes security requirements derived from the development phase (see Development Capability).

The Organization will ensure that the C&A (see the Risk Analysis Capability) and security requirements are understood, vetted, and approved by SSEs, ISSOs, Information Systems Security Managers (ISSMs), developers, C&A team, and stakeholders. This will take place prior to the deployment activities (e.g., plan, deploy, integrate/install and test, and follow up).

An Organization will plan for a deployment by performing a site survey. This site survey will consider the supporting infrastructure, physical environment, operational needs, user access to the site, and special equipment needs (e.g., transfer of cryptographic devices). An Organization will take into account special needs of protected sites (e.g., OPSEC).

An Organization will begin to deploy a solution to a site by notifying onsite personnel and following IA policies and procedures (e.g., collecting, storing, and processing data) before deployment. An Organization will inventory shipped applications, systems, and equipment (including unique equipment) and ship them to sites in accordance with Physical and Environmental Protections. Once the solution is received and deployed, the Organization will inventory the hardware and software assets as required by the Hardware Device Inventory and Software Inventory Capabilities.

An Organization will conduct integration/installation and testing onsite, which will be coordinated with onsite personnel. This process will be as automated, as possible, for updating and changing operational technologies and will be conducted by the deployment

team (e.g., SSEs, stakeholders, developers, ISSOs, ISSMs, and accrediting authorities). The Organization will employ C&A teams and ensure that solutions that are deployed have proper certifications.

An Organization will document and report a solution's statistics (e.g., risks, missing certifications) prior to operational use on the network. The reports will be provided to the ISSOs, ISSMs and the stakeholder who will either permit or deny a solution's deployment. An Organization will provide follow-on activities for a deployed solution that includes gathering information to be used for a capability performance goals assessment in the Portfolio Management Capability.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping–The Deployment Capability relies on the Network Mapping Capability to provide information about the current state of the network, which will be factored into deployment decisions made throughout the lifecycle.
- Hardware Device Inventory–The Deployment Capability relies on the Hardware Device Inventory Capability to provide a means for identifying hardware assets that are deployed on an Enterprise.
- Software Inventory–The Deployment Capability relies on the Software Device Inventory Capability to provide a means for identifying software assets that are deployed on an Enterprise.
- Architecture Reviews–The Deployment Capability relies on the Architecture Reviews Capability to evaluate systems for met and unmet security requirements.
- Risk Analysis–The Deployment Capability relies on the Risk Analysis Capability to provide the accreditation decision, which will impact deployment activities.
- Finance–The Deployment Capability relies on the Finance Capability to provide funding, including C&A funding, throughout the deployment lifecycle.

- Development—The Deployment Capability relies on the Development Capability to provide secure, tested solutions for deployment.

7.2   Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Deployment Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Deployment Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness—The Deployment Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Deployment Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Deployment Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3   Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- None

8   Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
PL-2 *SYSTEM*	Control: The organization:

SECURITY PLAN	b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. Enhancement/s: None Applicable.
SA-3 *LIFE CYCLE SUPPORT*	Control: The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities. Enhancement/s: None Specified.
SI-6 *SECURITY FUNCTIONALITY VERIFICATION*	Control: The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered. Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states include, for example, startup, restart, shutdown, and abort. Enhancement/s: (1) The information system provides notification of failed automated security tests. (2) The information system provides automated support for the management of distributed security testing. (3) The organization reports the result of security function verification to designated organizational officials with information

security responsibilities.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Deployment Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 801, Acquisition, 16 August 2009, Unclassified	Summary: National Intelligence Program (NIP) major system acquisitions (MSA) shall use the acquisition process model identified in Intelligence Community (IC) Policy Guidance (ICPG) 801.1 to ensure that a set of validated and approved requirements is implemented using a disciplined process through development, integration, and testing within an established schedule and budget.
ICPG 801.1, Acquisition, 12 July 2007, Unclassified	Summary: As directed in Intelligence Community Directive (ICD) 801, the IC acquisition approach will follow the Intelligence Community Acquisition Model (ICAM) and will be either a single-step development or, more frequently, an evolutionary development. Both single-step and evolutionary developments are characterized by discrete phases (e.g., concept refinement, development, production, deployment, and sustainment) that correspond to the maturity of a technical solution to meet validated user requirements.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 5000.01, The	Summary: Consistent with statute and the regulatory

Defense Acquisition System, 20 November 2007, Unclassified	requirements specified in this directive and in Department of Defense Instruction (DoDI) 5000.02, every Program Manager (PM) shall establish program goals for the minimum number of cost, schedule, and performance parameters that describe the program over its entire lifecycle. PMs shall consider supportability, lifecycle costs, performance, and schedule comparable in making program decisions. Planning for operation and support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system lifecycle.
DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008, Unclassified	Summary: This instruction implements Department of Defense Directive (DoDD) 5000.01 by establishing a simplified and flexible management framework for translating capability needs and technology opportunities based on approved capability needs, into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems. It describes the five phases of the Defense Acquisition Management System: Materiel Solution Analysis, Technology Development, Engineering & Manufacturing Development, Production & Deployment, and Operations & Support. Systems engineering shall be embedded in program planning and be designed to support the entire acquisition lifecycle.
DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified	Summary: This document establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DoD information systems. The process manages the implementation of information technology (IA) capabilities and services and provides visibility of accreditation decisions. The DIACAP requirements, activities, and tasks described are applicable throughout the information system's lifecycle, which includes deployment.
DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2007,	Summary: IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire lifecycle of the acquisition in accordance with an adequate

Unclassified	and appropriate Acquisition IA Strategy that shall be reviewed prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.
CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 December 2008, Unclassified	Summary: It is Joint Staff policy to ensure that DoD components develop, acquire, deploy, and maintain information technology (IT) and National Security Systems (NSS) that (1) meet the essential operational needs of U.S. forces; (2) are interoperable with existing and proposed IT and NSS through standards, defined interfaces, modular design, and reuse of existing IT and NSS solutions; … DoD combatant commands/services/agencies (C/S/A) play a key role in ensuring consistent interoperability is appropriately inculcated into the capability's lifecycle.
Defense Acquisition Guidebook, https://dag.dau.mil/Pages/ Default.aspx, 17 December 2009, Unclassified	Summary: This guidebook complements DoDD 5000.01 and DoDI 5000.02 by providing the acquisition workforce with discretionary best practices that should be tailored to the needs of each program. Section 4.3, Systems Engineering in the System Life Cycle, provides an integrated technical framework for systems engineering activities throughout the acquisition phases of a system's lifecycle, highlighting the particular systems engineering inputs, activities, products, technical reviews, and outputs of each acquisition phase.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Deployment Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP-800-64 Rev 2, Security Considerations in the System Development Life Cycle, October 2008, Unclassified	Summary: This special publication focuses on the information security components of the system development lifecycle (SDLC). It describes the key security roles and responsibilities that are needed in development of most information systems. Its scope is security activities that occur within the linear, sequential (a.k.a. waterfall) SDLC methodology. The five-step SDLC cited in this document (includes Deployment [as Implement]) is an example of one method of development and is not intended to mandate this methodology.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
ISO/IEC 15288:2008, Systems and Software Engineering–System Life Cycle Processes, 1 February 2008,	Summary: This document provides a common process framework and the processes for acquiring and supplying systems. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the full system lifecycle

Unclassified	(e.g., conception of ideas, development, production, utilization, support, and retirement of the system) and to the acquisition and supply of systems.
IEEE 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process, 9 September 2005, Unclassified	Summary: This standard defines the interdisciplinary tasks that are required throughout a system's lifecycle to transform stakeholder needs, requirements, and constraints into a system solution. It is intended to guide the development of systems for commercial, government, military, and space applications and applies to projects within an Enterprise that is responsible for developing a product design and establishing the lifecycle infrastructure needed for lifecycle sustainment.
International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, version 3.1, 2007, Unclassified	Summary: This handbook describes the key process activities performed by systems engineers, covering in detail the purpose for each process activity, what needs to be done, and how to do it. It provides sufficient information to determine whether a given process activity is appropriate in supporting program objectives and how to go about implementing the process activity.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Deployment logistics–The number, location, and methods used for deployment will affect its cost.
2. Considerations for deployment made during development–Developers may or may not have made considerations to facilitate deployment actions.
3. Complexity of solutions to be deployed–Complex solutions may require more resources and time to deploy.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Deployment Capability.

- The Enterprise shall be responsible for the incorporation of IA throughout the deployment phase of the lifecycle and is responsible for modifying and maintaining an operational baseline in accordance with mission needs.
- The Enterprise shall coordinate security expertise and collaboration with the SSEs, stakeholders, and developers who ensure that the C&A activities and security requirements are defined to meet deployment IA objectives.
- The Enterprise shall coordinate with ISSOs who shall be responsible for updating systems security plans (SSPs) and ensuring the overall security deployment.
- The SSEs shall ensure development, integration, and test personnel deploy systems securely by understanding the testing that was performed and the results, and understanding the changes that were made to the solution based on those test results.
- The Enterprise shall have IT support onsite at the time of deployment to ensure the process is executed properly.
- All personnel shall have IA background and knowledge such that they can coordinate with the SSEs and ensure that the C&A and security requirements are understood, vetted, and accepted by the developers and security stakeholders.
- The Enterprise shall employ services from a program management role or office to ensure that all activities and resources are managed according to the program management plan and are able to meet the established IA objectives.
- Program management shall provide visibility into the deployment activity of other programs with dependencies on the deployment activity.

- The Enterprise shall use the approved lifecycle process that is established by policy, procedures, and standards.
- The Enterprise shall perform a site survey to ensure that the site is prepared for a deployment.
- Site surveys shall be performed for large and small deployment environments.
- Deployment considerations shall include the necessary supporting infrastructure, such as space, power, and cooling, among other physical and environmental considerations.
- The Enterprise shall ensure that deployment personnel have been trained for the solution that is being deployed at the operational site and that access needs and POCs have been identified.
- The Enterprise shall take special considerations when deploying cryptographic devices and other specialized equipment.
- The Enterprise shall use methods and accounting procedures as defined by the Enterprise's IA policy, procedures, and standards to transfer specialized equipment.
- The Enterprise shall deploy the systems in accordance with OPSEC policies or the policies uniquely defined for the sensitive systems.
- The Enterprise shall consult with ISSOs and officials from the deployment site for security decisions including the use of cover terms when deploying protected systems.
- The Enterprise shall provide early notification to the deployment site, customers, and owners of a scheduled solution for deployment.
- The Enterprise shall ensure that policies for collecting, storing, and processing data are in place before deployment occurs.
- The Enterprise shall ensure that deployment resources and methods of deployment are defined and review currently deployed corporate services to ensure corporate services are leveraged where appropriate and to ensure redundant services are not deployed.
- The Enterprise shall ensure that deployed systems are inventoried and provided shipping protections as well as use confirmation of inventory upon receipt to the deployment site.
- Systems shall be shipped to the deployment site in accordance with physical and environmental protection requirements.
- The Enterprise shall perform a pre-ship review and shipping audits.

- Stakeholders and security personnel shall approve the shipment prior to transfer for deployment to ensure that all documentation, test results, discrepancy reports, permits, and certifications are in order.
- The pre-ship review and shipping audits shall have authorized approval for operation after deployment to the site.
- ISSOs shall be consulted for security decisions when deploying systems.
- The Enterprise authorities and stakeholders shall make the final decision as to whether a solution will be deployed.
- The Enterprise shall include deployment documentation of the oversight and compliance requirements including any external measures and metrics.
- Deployed systems shall be coordinated with C&A activities and ultimately timed with the accreditation decision.
- The C&A team shall report when systems are in danger of deploying without certain certifications.
- Stakeholders shall make any risk decisions based on the available information and the mission needs.
- The Enterprise shall provide an operational mechanism that is certified and accredited for the Enterprise.
- An operational site for deployment shall include integration, installation, and, whenever feasible, testing at the operational site.
- Testing shall occur during deployment when feasible to ensure that a deployed solution is functional and does not compromise the mission flow of an Enterprise.
- If a deployed solution fails testing, procedures for uninstalling shall be defined, documented, and used to remove the solution or disable the solution for use on the Enterprise.
- The Enterprise shall keep software and hardware assets up to date once the solution is received and deployed at the site.
- All deployed assets shall be configurable to be discoverable by automated means for updating and upgrading operational technologies on the Enterprise.
- During post-deployment, the deployed solution shall be evaluated against the performance goals defined by the Enterprise portfolio to determine whether the solution is operating effectively for the mission needs of the Enterprise.